8

16 December 1983

MEMORANDUM FOR: Chairman, Information Systems Board

FROM: Computer Security Working Group

SUBJECT: Reaction to the Workstation Environment
Working Group's Interim Report Dated
25X1 16 November 1983 [redacted]

1. The Computer Security Working Group has reviewed the Workstation Environment Working Group's (WSEWG) Interim Report of 16 November 1983. We recommend that the WSEWG vigorously pursue its recommended approach for the near-term solution of the Agency's VDT requirements. It should also continue its assessment of the Agency's long-term needs and establish a firm goal for realizing the full set of combined capabilities. This Agency has pushed the state-of-the-art before and there is a need to do
25X1 it again. [redacted]

2. We are concerned, however, that the unlimited procurement of numerous types of personal computers will seriously impact the Agency's security and communications security programs. The proliferation of microcomputers in recent years has already made it impossible to evaluate the security vulnerabilities of more than a few of these devices. The WSEWG inventory indicates that 219 PC's were procured for the Agency during FY-82/83 from a total of 22 different manufactures (and
25X1 this is probably a conservative estimate). [redacted]

3. Experience has shown that information systems security and communications security concerns are often specific to the hardware, software, and firmware of an individual model of a particular manufacturer. A review of the Wang Alliance system, for example, took some six months and cost $120,000 -- and the test results were applicable only to a standard Alliance/OIS
25X1 configuration. [redacted]

4. Similarly, there is an ongoing project within COMSEC to investigate both Data Encryption Standard and high level encryption routines for microcomputers. These initiatives are also hardware and software specific and should logically also be
25X1 focused on a minimum number of types. [redacted]

5. Of related concern are the dual problems arising from the local archiving and local programming capabilities of many microcomputers. By providing single or dual disk drives, these PC's allow the user to copy data on magnetic media; thereby

25X1 [redacted]

defeating an important element of the audit trail system. Furthermore, by writing and executing programs locally, a sophisticated user can bypass many (in some cases all) of the security controls. While these vulnerabilities can be controlled, the fixes are again specific to the hardware, software and firmware configuations. Once again, the more types of equipment introduced, the more difficult it becomes to "fix" each one. [redacted] 25X1

6. We recommend that the final draft of the WSEWG report take note of the fundamental security vulnerability created by uncontrolled diversity; and suggest that it call for a rational limit to the number of "testbeds" utilizing unique PC's and microcomputing peripherals. We believe that four to six different manufacturers would represent a healthy balance between too few PC's to allow for valid comparisons and so many devices that no group -- Logistics, Security, Communications, or Data Processing, -- could properly support them. [redacted] 25X1

25X1 [redacted]